

## UNITED STATES DISTRICT COURT

FILED

SEP 27 2024

for the

Northern District of Oklahoma

Heidi D. Campbell, Clerk  
U.S. DISTRICT COURT

In the Matter of the Search of )  
 Lenovo Thinkbook Laptop S/N MP23MOEW, )  
 Currently Stored at BIA/OJS Miami Agency Evidence Pod )  
 in Miami, Oklahoma )

Case No. 24-MJ-601-CDLFILED UNDER SEAL

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 1344  
 18 U.S.C. § 1349  
 18 U.S.C. §§ 1028 and 1028A  
 18 U.S.C. §§ 371

Bank Fraud  
 Attempt and Conspiracy  
 Aggravated Identity Theft  
 Conspiracy

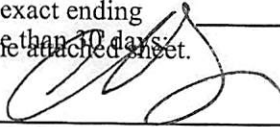
The application is based on these facts:

See Affidavit of Charles Carroll, BIA Special Agent, attached hereto.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_

\_\_\_\_\_ days (give exact ending date if more than 30 days) is requested  
 under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


  
 Applicant's signature

Charles Carroll, BIA Special Agent  
 Printed name and title

Subscribed and sworn to by phone.

Date: September 27, 2024

City and state: Tulsa, Oklahoma

  
 Judge's signature

Christine D. Little, U.S. Magistrate Judge  
 Printed name and title

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**IN THE MATTER OF THE SEARCH  
OF:  
LENOVO THINKBOOK LAPTOP S/N  
MP23MOEW,**

Currently Stored at BIA/OJS Miami  
Agency Evidence Pod in Miami, OK.

Case No. \_\_\_\_\_

**FILED UNDER SEAL**

**Affidavit in Support of an Application  
Under Rule 41 for a Warrant to Search and Seize**

I, Charles Carroll, being first duly sworn, hereby depose and state as follows:

**Introduction and Agent Background**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property – an electronic device described in Attachment A, which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

Specifically, I am a Special Agent with the Bureau of Indian Affairs (BIA), Branch of Criminal Investigation, assigned to the BIA's Oklahoma City Field Office. I

have been a Special Agent with the BIA since May 2013. I have received training in interviewing and interrogation techniques, arrest procedures, search and seizure, computer crimes, intellectual property and other white-collar crimes, search warrant applications, conducting physical surveillance, conducting short- and long-term undercover operations, consensual monitoring, analyzing telephone and electronic pen register and caller identification, system data, basic narcotics investigations, drug identification, detection, interdiction, United States narcotics laws, financial investigations, identification and seizure of drug related assets, undercover operations, and electronic and physical surveillance procedures at the Federal Law Enforcement Training Centers (FLETC) in Glynco, GA.

3. In addition to basic law enforcement training, I have also received training in the following areas: criminal use of email, social media, and telephonic communications, computer-related crime, FBI Crimes Against Children Online Undercover Operations, law, investigative techniques, surveillance, tactics, and firearms, the daily work related to conducting these types of investigations, interviewing and interrogation techniques, arrest procedures, search and seizure, computer crimes, intellectual property and other white-collar crimes, search warrant applications, conducting physical surveillance, conducting short- and long-term undercover operations, consensual monitoring, analyzing telephone and electronic pen register and caller identification, system data, basic narcotics investigations, drug identification, detection, interdiction, United States narcotics



laws, financial investigations, identification and seizure of drug related assets, undercover operations, electronic and physical surveillance procedures.

4. I have been assigned to the FBI Ardmore/Durant Safe Trails Task Force, a joint federal and local task force investigating violations of federal law committed by criminal street gangs and other violent criminal organizations in Indian Country. Prior to joining the Bureau of Indian Affairs, I worked with City of Atoka Police Department as a CLEET Certified Peace Officer for approximately 8 years.

5. I have experience with cases involving the following crimes: aggravated identity theft, assault with a deadly weapon inflicting serious injury, crimes against children, criminal investigations, cyber investigations, drug trafficking, electronic surveillance methods, false reports of bomb threats and other hoaxes designed to elicit a law enforcement response, felon in possession of a weapon, financial crimes, firearms offenses, fugitives, Indian country, individuals who communicate and coordinate electronically, internet fraud, kidnapping, mail fraud, money laundering, narcotics trafficking, physical and electronic surveillance, reviewing financial records, robbery, sexual abuse material, the receipt, possession, production, advertisement, and transmission of child sexual abuse materials, traffic violations, violations of Title 18 of the United States Code, violent crime, violent fugitives, violent gangs, and wire fraud.

6. I also have experience utilizing the following investigative techniques and procedures: arrest warrants, consensual monitoring, debriefing of defendants,

informants, and witnesses, examining digital evidence related to financial crimes cases, executing search warrants, identification and collection of computer-related evidence, interviewing suspects, victims, and witness, search and seizure of computers, computer equipment, software, and electronically stored information, search and seizure warrants, search warrants for online accounts and electronically stored information ("ESI"), surveillance, use of confidential informants, and information obtained from other agents, witnesses, and agencies.

7. In addition to my basic law enforcement training at the Federal Law Enforcement Training Centers (FLETC), I have also received training in the following areas: criminal use of email, social media, and telephonic communications, computer-related crime, FBI Crimes Against Children Online Undercover Operations, law, investigative techniques, surveillance, tactics, and firearms, the daily work related to conducting these types of investigations, interviewing and interrogation techniques, arrest procedures, search and seizure, computer crimes, intellectual property and other white-collar crimes, search warrant applications, conducting physical surveillance, conducting short- and long-term undercover operations, consensual monitoring, analyzing telephone and electronic pen register and caller identification, system data, basic narcotics investigations, drug identification, detection, interdiction, United States narcotics laws, financial investigations, identification and seizure of drug related assets, undercover operations, and electronic and physical surveillance procedures.

8. I am an “investigative or law enforcement officer” within the meaning of 18 U.S.C. § 2510; that is, an officer of the United States of America who is empowered to investigate and make arrests for offenses alleged in this warrant. Specifically, as part of my duties as a Special Agent for the Bureau of Indian Affairs, I investigate crime in Indian Country, including the violations alleged in this application for a Search Warrant.

9. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based in part on information provided by other law enforcement officers and on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary for the limited purpose of establishing probable cause to conduct a search of and for the items described in Attachments A and B for evidence, contraband, and/or instrumentalities of the criminal conduct described herein. Additionally, unless otherwise indicated, wherever in this Affidavit I assert that an individual made a statement, that statement is described in substance herein and is not intended to be a verbatim



recitation of such statement. Furthermore, unless otherwise indicated, all statements contained in this Affidavit are summaries in substance and in part.

10. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 1344 (Bank Fraud); 18 U.S.C. § 1349 (Attempt and Conspiracy); 18 U.S.C. §§ 1028 and 1028A (Aggravated Identity Theft); and 18 U.S.C. § 371 (Conspiracy), will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

#### **Identification of the Device to be Examined**

11. The property to be searched is a Lenovo Thinkbook laptop, serial number MP23MOEW, hereinafter the "Device." The Device is currently located at BIA/OJS Miami Agency Evidence Pod Miami, OK.

12. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

#### **Jurisdiction**

13. "[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a.

14. The requested search is related to the following violations of federal law:

18 U.S.C. § 1344 (Bank Fraud);

18 U.S.C. § 1349 (Attempt and Conspiracy);  
18 U.S.C. §§ 1028 and 1028A (Aggravated Identity Theft); and  
18 U.S.C. § 371 (Conspiracy).

15. Venue is proper because the person or property described in this affidavit is within the Northern District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

### **Probable Cause**

#### *Fraudulent Checks*

16. On August 17, 2023, at approximately 11:30 a.m., Miami, OK Police Department Officer Jeremy Myers went to Courtesy Loans, 1510 N. Main Street Miami, Oklahoma, within the City Limits of Miami, OK, within the Northern District of Oklahoma, for a report of fraudulent checks. Officer Myers spoke with Courtesy Loans employee Patricia Burton (Burton). Burton said the Courtesy Loans' financial institution, First National Bank, notified her that the business account was overdrawn. Burton checked the account and found several checks drawn on Courtesy Loan's account that were duplicated and not written by any employee of Courtesy Loans. The signature line of the checks showed a signature purporting to be that of Valerie Odell, who is an employee of Courtesy Loans, but Odell did not write or sign the referenced checks.

17. On August 17, 2023, at approximately 2:20 p.m., Officer Myers went to First National and Trust Company of Miami, Oklahoma based on the report of someone attempting to cash a fraudulent check. Bank personnel told Officer Myers that the subject, Joshua Cole (Cole), was in a gray pick-up truck sitting in



the drive-through. As Officer Myers pulled on the scene, he saw a gray truck in the parking area of the bank, and a male got out of the vehicle and walked into the bank. The gray truck then left the area. Bank staff directed the officer to a male identified as Joshua Cole at the teller counter. Officer Myers handcuffed Cole and read him his Miranda Rights. Cole refused to answer questions without an attorney and was released. Another Miami Police Officer was able to locate and conduct a traffic stop on the vehicle that dropped Cole off at the bank. The driver, Henry Foote (Foote), told officers he didn't know Cole and that Taylor Zabel asked him to give Cole a ride to the bank.

18. On August 21, 2023, Miami Police Detective David Wright was assigned to investigate the check fraud case. Detective Wright viewed bank surveillance video of several of the fraudulent checks being cashed. Detective Wright identified the subjects involved using investigative techniques and his prior dealings with the subjects. Detective Wright noticed Zabel as being involved in most of the activity. According to the bank surveillance video, on August 7, 2023, Zabel cashed check # 00002313 in the amount of \$400.00 and, on August 11, 2023, Zabel cashed check #00002358 in the amount of \$900.00.

19. On August 30, 2023, Courtesy Loans employee Patricia Burton sent an email to Det. Wright listing the fraudulent checks and the account to which they are attached. Burton wrote:

CK# 2313 TAYLOR ZABEL \$400 546 RHONDA JOHNSON 8/7/23 3:30 PM  
CK# 2326 SAMULE CONRAD \$700 546 RHONDA JOHNSON 8/8/23 11:21 AM  
CK#2335 TIFFANY TUSH \$900 OLEN TYREL THORNBURY (TY) 8/9/23 8:16 AM

CK#2347 RHONDA JOHNSON \$900 546 RHONDA JOHNSON 8/9/23 1:02 PM  
CK#2348 TIFFANY INGRAM \$900 546 RHONDA JOHNSON 8/9/23 4:58 PM  
CK#2354 SAMULE CONRAD \$900 506 BRANDEE HORSECHIEF 8/10/23 2:50 PM  
CH#2358 TAYLOR ZABEL \$900 546 RHONDA JOHNSON 8/11/23 11:04 AM  
CH#2369 MATTHEW WRIGHT \$900 546 RHONDA JOHNSON N/A  
CH#2370 SAMULE CONRAD \$900 546 RHONDA JOHNSON 8/15/23 4:26 PM  
CH#2371 MELVIN SMITH \$900 546 RHONDA JOHNSON 8/16/23 1:59 PM  
CH#2374 JOSHUA COLE \$700 546 RHONDA JOHNSON 8/17/23

Burton indicated that all of that checks were cashed at the same location and all by the same teller except check # 2354.

Laptop at the Pawn Shop

20. On September 6, 2023, Detective Wright received information that Zabel pawned a laptop, and more specifically, a Lenovo Thinkbook S/N MP23MOEW ( the "Device), at Hometown Pawn, 410 N. Main Street Miami, Oklahoma. Detective Wright printed the pawn ticket, #8661, using "Leads Online" software. The computer was turned over to the Miami Police Department by Hometown Pawn. Detective Wright later turned the Device over to the BIA.

21. On November 13, 2023, Detective Wright interviewed one of the subjects involved, Jade Uto (Uto), at the Miami Police Department Detective Office. Uto was read her Miranda Rights and she agreed to answer questions. Uto said she obtained the check she cashed from Zabel. Uto said she was visiting Zabel and told her she needed to make some money to pay bills. Zabel said she could probably help her. Uto said she was to cash the \$900.00 check and keep \$300.00 and give the remaining \$600.00 to Zabel. Uto said Lisa Busby gave her a ride to the bank, although she claimed Busby did not know anything about the fraudulent check. When asked how Zabel got the checks, Uto said "a

printer.” Uto said she was going to cash another one but learned that Cole had gotten caught.

22. On November 20, 2023, Detective Wright interviewed Rhonda Johnson (Johnson) at the Miami Police Department Detective Office. Johnson was read her Miranda Rights and agreed to answer questions. Johnson said Zabel provided her with the check she cashed and Johnson identified Zabel as being in the vehicle with her while she cashed it. Johnson said Zabel had asked her about cashing some checks. Johnson told Detective Wright that Zabel was the one who made the check using banking information from a loan proceeds check she received from Courtesy Loans.

23. Detective Wright learned that most of the subjects involved in his investigation had Indian status or Indian citizenship. Zabel is enrolled in the Cherokee Nation of Oklahoma, and the crime was committed within Indian Country. Detective Wright requested assistance from the BIA Branch of Criminal Investigation.

24. On September 4, 2024, I spoke with Alton Carney (Carney), manager of Hometown Pawn, in Miami, Oklahoma. Carney said on September 6, 2023, Zabel and a male identified as Matthew Wright came into the shop to pawn a laptop computer. Carney said as standard procedure before taking in a computer, he powered it on and asked Zabel for the password. Zabel provided the password. As soon as the home screen came up, Carney observed what he described as different levels or windows, of checks that were being typed. Some



of the checks had part of the writing erased. Carney said the checks were written to different people and different businesses. I asked Carney if this could have been an online banking program and he said, "no," it was not like online banking.

25. The Device is currently in the lawful possession of the BIA. It came into the BIA's possession in the following way: Hometown Pawn suspected the Device to have been used in criminal activity and turned it over to the Miami Police Department. Therefore, while the BIA might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

26. The Device is currently in storage at BIA/OJS Miami Agency Evidence pod. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the BIA.

### **Technical Terms**

27. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

- A. "Digital device," as used herein, includes the following three terms and their respective definitions:

- i. A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. See 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.
- ii. “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.
- iii. “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives,

floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- B. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- C. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other



digital form. It commonly includes programs to run operating systems, applications, and utilities.

D. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

E. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

### **Electronic Storage and Forensic Analysis**

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of

time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- A. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- C. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who

has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

D. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

30. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium



that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- B. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- C. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- D. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information

necessary to understand other evidence also falls within the scope of the warrant.

- E. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- F. I know that when an individual uses an electronic device to alter, create, make, use, produce, possess, or transfer false or otherwise fraudulent documents or means of identification of another person, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

31. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that

might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

33. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is



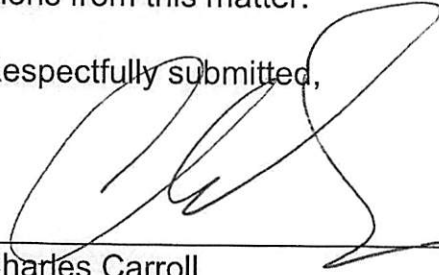
reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### Conclusion

34. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

35. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,



Charles Carroll  
Special Agent,  
Bureau of Indian Affairs

Subscribed and sworn to by phone on September 27, 2024.



---

CHRISTINE D. LITTLE,  
UNITED STATES MAGISTRATE JUDGE

## **ATTACHMENT A**

### **Property To Be Searched**

The property to be searched is a Lenovo Thinkbook laptop computer, serial number MP23MOEW, hereinafter the "Device." The Device is currently located at BIA/OJS Miami Agency Evidence Pod, Miami, OK.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

## **ATTACHMENT B**

### **Particular Things to Be Seized**

All records on the Device described in Attachment A that relate to violations of the following crimes:

18 U.S.C. § 1344 (Bank Fraud);  
18 U.S.C. § 1349 (Attempt and Conspiracy);  
18 U.S.C. §§ 1028 and 1028A (Aggravated Identity Theft); and  
18 U.S.C. § 371 (Conspiracy)

involving the following suspects:

Taylor Zabel  
Mathew Wright  
Shawn Barr  
Jade or Jayde Uto  
Rhonda Johnson or Rhonda Watkins  
Tiffany Ingram  
Samule Conrad  
Brandee Horsechief  
Melvin Smith  
Joshua Cole  
Tiffany Tush  
Olen Tyrel Thornbury  
Lisa Busby  
Henry Foote

hereinafter, the "Suspects," as described in the search warrant affidavit, including, but not limited to:

### **Offense Records**

1. Records relating to documentation or memorialization of the criminal offenses listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos, including device



information, geotagging information, and information about the creation date of the audio and video media;

2. Records relating to the planning and execution of the criminal offenses above, including Internet activity, firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;
3. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above;
4. Records relating to communications as to the criminal offenses listed above; including emails; applications that serve to allow parties to communicate; any type of voice, text or multimedia messages; all call logs; and other Internet-based communication media;
5. Any items in the names of the First National Bank and Trust Company of Miami, Oklahoma or Courtesy Loans in Miami, Oklahoma, and any other business or individual associated, which demonstrates the giving or receiving of funds from the First National Bank and Trust Company of Miami, Oklahoma or Courtesy Loans in Miami, Oklahoma;
6. Bank records, including signature cards, bank statements, deposit slips, checks deposited, checks drawn on the account, records pertaining to all debit and credit memos, Forms 1099 issued, wire transfers, cashier's checks, money orders and canceled checks for any and all bank accounts, including

all funds on deposit such as certificates of deposit and money market accounts, and safety deposit box rental receipts;

7. Loan records, including applications, financial statements, loan collateral, credit and background investigations, loan agreements, notes or mortgages, settlement sheets, contracts, checks issued for loans, repayment records, including records revealing the date, amount and method of repayment (cash or check), checks used to repay loans and a record disclosing the total amount of discount or interest paid annually, records of any liens, loan correspondence files, and internal bank memoranda;

8. Accounting records, specifically financial statements, ledgers, journals, check registers, notes, correspondence and other books and records of the Suspects;

9. Documentation or receipts of personal or business expenditures, including but not limited to credit card statements;

10. Records relating to electronically stored tangible items evidencing the obtaining, transfer, secreting, or concealment of assets or money;

11. Electronically stored records, documents, receipts, or negotiable instruments which evidence the purchase of negotiable instruments or the structuring of currency transactions to avoid the filing of currency transactions reports or the laundering of monetary instruments;

12. Electronically stored documents evidencing fruits, instrumentalities, monies, records, and notations, associated with the crimes listed above.

### **Technical Device Records**

13. Records and information related to the geolocation of the and travel in furtherance of the criminal offenses listed above from June 27, 2023 to September 6, 2023, which represents the approximate time period in which the Suspects may have planned or engaged in the criminal offenses;
14. Evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
15. Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
16. Evidence of the lack of such malicious software;
17. Evidence indicating how and when the Device was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
18. Evidence indicating the Device user's state of mind as it relates to the crime under investigation;
19. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;



20. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;
21. Evidence of the times the Device was used;
22. Passwords, encryption keys, and other access devices that may be necessary to access Device applications;
23. Documentation and manuals that may be necessary to conduct a forensic examination of the Device;
24. Records of or information about the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
25. Contextual information necessary to understand the evidence described in this attachment;
26. Records of or information about Internet Protocol addresses used by the Device;
27. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such

as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

### **Search Procedures for the Device**

In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

- a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 90 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 90-day period without obtaining an extension of time order from the Court.
- b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.
- c. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search

for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

- d. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.
- e. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.
- f. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.
- g. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.
- h. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.



- i. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.